УДК 681.3.06

ЗАСТОСУВАННЯ АЛГОРИТМУ КОЛОНІЇ МУРАХ ДЛЯ КРИПТОАНАЛІЗУ ШИФРІВ ПЕРЕСТАНОВКИ

Куровець Б.І.

Гриник Р.О., ЛДУ БЖД, викладач КУІБ

ЛДУ БЖД

В останні роки інтенсивно розвивається новий науковий напрям який використовує математичні методи які містять принципи природних механізмів прийняття рішення, даний напрям називають «Природні обчислення». Напрям об'єднює в собі такі розділи як еволюційні алгоритми, обчислення з допомогою нейронних мереж, алгоритми ройового інтелекту та алгоритм мурашиних колоній. В [1,2] розглядаються методи атак на традиційні симетричні алгоритми з використанням інтелектуальних систем побудованих на еволюційних алгоритмах оптимізації.

Основною ознакою класу шифрів перестановки є те що символи відкритого тексту при шифруванні тільки міняються місцями між собою за певним правилом. У загальному випадку результатом роботи таких шифрів є криптограма котра містить тільки ті символи котрі містяться у відкритому тексті тільки у зміненому порядку. З цього випливає, що задача крипто аналізу полягає у визначенні позиції для призначення символів криптограми таким чином, щоб цільова функція, яка визначає оптимальність вихідного повідомлення, досягла свого екстремуму. Тобто дана задача зводиться до часткового випадку «Задачі про призначення», яка є однією з базових задач комбінаторної оптимізації і полягає в знаходженні парування мінімальної (або максимальної) ваги між елементами двох скінчених множин. Вона може бути подана як знаходження парування у зваженому дводольному графі [3]. Задачу про призначення можна сформулювати наступним чином: присвоємо $X_{ij} = 1$, якщо об'єкт i призначений в пункт j, і $X_{ij} = 0$ в іншому випадку, C_{ij} - витрати на передачу обсягу ресурсів з пункту i в пункт j. В цьому випадку модель оптимызації буде мати наступний вигляд:

$$R_{i=1}^{n} = \sum_{j=1}^{n} \sum C_{ij} X_{ij} \rightarrow \text{екстр},$$

де n – число об'єктів та місць їх розташування.

Якщо застосувати дану модель до задачі криптоаналізу потокового шифру, то необхідно вважати, що C_{ij} - ймовірність того, що за символом в позиції i повинен слідувати символ в позиції $i+1$, крім цього необхідно ввести параметр Q_i, який буде відповідати за осмисленість тексту. В такому випадку наша оптимізаційна модель буде мати наступний вигляд:

$$R = \sum_{i=1}^{n} \sum_{j=1}^{n} Q_i C_{ij} X_{ij} \rightarrow max.$$

Таким чином, загальне значення цільової функції R, отримане в кожному конкретному варіанті призначення символів в позиції, може бути визначено як довжина маршруту котрий з'єднує вибрані елементи, тобто:

$$R = \sum_{\substack{i=1,\dots,n-1 \\ j=2,\dots,n}} C_{ij}.$$

Очевидно, маршруту з великим значенням R повинна відповідати більш висока концентрація феромону F, яка використовується в якості ймовірності вибору чергового маршруту та представляє черговий варіант призначення позиції для символу.

Задача криптоаналізу буде вирішуватись у шість етапів:

1. Випадковим чином обирається задана кількість m варіантів маршрутів і обчислюються значення фітнес-функцій $R_1, R_2, \dots, R_m$.
2. Комбінаціям ik_1 розміщення символів k присвоюють ваговий коефіцієнт.
3. Для кожної комбінації ik обчислюється концентрація феромону F_{ik}.
4. Проводиться імітація випаровування феромону з комбінацій ik по яким пройшли мурахи.
5. Після визначення нової кількості феромону виконується повернення мурах в початкові позиції і визначається ймовірність розміщення символу k в позиції i у новому маршруті P_{ik}.
6. У відповідності з P_{ik} формується $d * m$ нових маршрутів ($d < 1$), для котрих обчислюється значення фітнес-функцій, після чого проводиться вибірка із m кращих варіантів. Якщо оптимальне значення фітнес-функції не змінюється протягом декількох ітерацій то пошук маршруту закінчується, в іншому випадку довжина маршруту обнулюється і проводиться повернення до другого кроку.

З вище сказаного можна зробити висновок, що комбінування алгоритму мурашиних колоній з алгоритмом вирішення задачі про призначення може істотно підвищити ефективність та швидкість вирішення задачі по крипто аналізу шифрів перестанови.

ЛІТЕРАТУРА

1. Сергеев А.С. Исследование возможности организации криптографической атаки с использованием эволюционной оптимизации и квантового поиска при разработке систем передачи и защиты информации / А.С. Сергеев // Теоретические и прикладные вопросы современных информационных технологий: материалы 6-й всерос. науч.-техн. конф. – Улан-Удэ: Изд-во ВСГТУ, 2005. – С.61-65.

2. Сергеев А.С. Применение методов генетического поиска для организации криптоанализа блочных криптосистем на примере стандарта шифрования DES / Сергеев А.С.

// Научная мысль Кавказа. Прил. – Ростов н/Д: Изд-во СКНЦ ВШ. – 2006. – №15. – С.185-193.

3. Задача про призначення [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/ Задача_про_призначення